Cyren Sandboxing

Enterprise Security SaaS

Stoppen Sie schwierig zu erkennende Zero-Day-Bedrohungen mit dem Sandbox-Array von Cyren in der Cloud

Die Cyberbedrohungen von heute entwickeln sich ständig weiter. Ihr Unternehmen ist Zero-Day-Exploits, zielgerichteten Angriffen und anhaltenden Bedrohungen wie es sie noch nie zuvor gegeben hat, ausgesetzt. Diese Bedrohungen sind speziell darauf ausgerichtet herkömmliche Malware-Verteidigungslinien und Sandboxen der ersten Generation zu durchdringen. Kein Unternehmen ist immun. Attacken wirken sich auf Unternehmen jeder Größe und Branche aus. 60 % aller zielgerichteten Angriffe richten sich auf kleine und mittelständische Unternehmen.

Zero-Day-Schutz mit innovativem Cloud-Sandbox-Array

Cyren Sandboxing schützt Ihr Unternehmen vor Verletzungen und Datenverlust durch die schwer zu erkennenden Zero-Day-Bedrohungen von heute mithilfe einer benutzerfreundlichen und kosteneffektiven Cloud-Lösung. Basierend auf dem branchenweit ersten Cloud-Sandbox-Array analysiert Cyren Sandboxing verdächtige Dateien und URLs, auf die Ihre Benutzer in E-Mails oder im Internet zuzugreifen versuchen. Wenn wir eine neue Bedrohung identifizieren, implementieren wir sofort Schutzmaßnahmen für alle Benutzer im gesamten Cyren-Netzwerk, indem wir die identifizierten bösartigen Dateien, URLs und den Befehl- und Steuer-Traffic blockieren.

Skalierbarer Schutz für alle Benutzer und den gesamten Web-Traffic einschließlich SSL

Die Bedrohungen und APT-Angriffe von heute nutzen unter vielen anderen Methoden zunehmend schwer zu erkennende Techniken, die prüfen, ob sie in einer virtuellen Sandbox ausgeführt werden, und dann ihr Verhalten ändern, um nicht entdeckt zu werden. Da die Angriffe immer ausgefeilter werden, überwinden sie die Verarbeitungs- und Architektur-Beschränkungen herkömmlicher Appliances mit relativer Leichtigkeit.

Cyren Sandboxing ist darauf ausgelegt, alle Ihre Benutzer zu schützen, von Mitarbeitern unterwegs bis zu Niederlassungen und dem Hauptsitz. Dies erfolgt aus der Cloud heraus, wo unsere massiv skalierbare Sicherheitsplattform bereits mehr als 17 Milliarden Internet- und E-Mail-Transaktionen pro Tag verfolgt und die schnellste Bedrohungsanalyse sowie die höchsten Erkennungsraten bietet. In unserer vereinheitlichten, globalen Sicherheits-Cloud können elastische Computing-Ressourcen echte Verhaltensanalysen durchführen, die notwendig sind, um eine Bedrohung zu erkennen. Dies umfasst die zusätzliche Verarbeitungslast der vollständigen Prüfung von, in verschlüsseltem SSL-Traffic verborgenen, Bedrohungen.

Integrierte Sicherheits-Layer in einer Cloud-Plattform – einfach einschalten

Cyren Sandboxing wird als integrierter Bestandteil unserer mehrschichtigen Sicherheits-Cloud geliefert. Das bedeutet eine sofortige Bereitstellung und vollständige Synergie zwischen dem Sandboxing-System und anderen Layers wie z. B. eine dynamische Analyse des Rufes eines Unternehmens im Internet. Als cloudbasierte SaaS gibt es keine zeitaufwendigen Updates und Sie führen stets die neueste Version aus.

CYREN SandBoxing

Der Cloud Sandbox Array-Unterschied

Die zum Patent angemeldete Sandbox Array-Technologie von Cyren ist ein fundamentaler Schritt im Kampf gegen immer invasivere Malware und bietet:

Hervorragende Detektion

- Unser cloudbasiertes Array stellt Dateien nicht nur in verschiedenen Umgebungen sondern auch für unterschiedliche Sandbox-Typen zur Verfügung, die sowohl auf virtuellen als auch auf physischen Rechnern ausgeführt werden.
- Cyren hat den komplexen Prozess der Dateianalyse, der in der Regel manuell durch Malware-Rechercheure durchgeführt wird, automatisiert, was zu besseren Analysen und fundierten Zero-Day-Bedrohungsinformationen führt.

Unbeschränkte Skalierbarkeit

- Weil sich das Sandbox Array von Cyren in der Cloud (und nicht auf einer Appliance) befindet, ist die Skalierung ein Kinderspiel. Es werden einfach mehr Maschinen und Ressourcen genutzt, wenn dies erforderlich wird.

Schnellere Analyse

- In vielen Fällen kann das Risikoprofil einer Datei noch vor der eigentlichen dynamischen Analyse beim Sandbox-Start bestimmt werden.

Umfassendere Berichtsdaten

- Obgleich wir eine Datei mithilfe verschiedener Sandbox-Typen analysieren können, bieten wir einen einzigen, vereinheitlichten Bericht und Risiko-Score. Die im Bericht angegebenen Informationen umfassen die zusammengeführte Liste der Risiken, die in den, in verschiedenen Umgebungen durchgeführten, Analysen beobachtet wurden.

www.cyren.com/**contact**

Mehr als 500.000
BEDROHUNGSERKENNUNGSPUNKTE

Mehr als 600 Mio.
GESCHÜTZTE BENUTZER

Mehr als 17 Mrd.
TÄGLICHE TRANSAKTIONEN

Mehr als 130 Mio.
ABGEWEHRTE BEDROHUNGEN

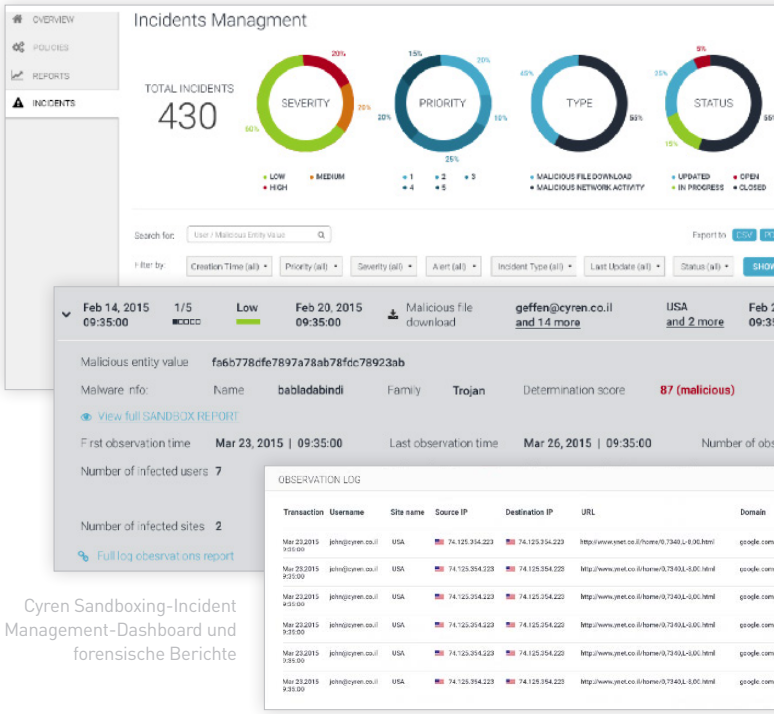
CYREN

CYREN SANDBOXING

Enterprise Security SaaS

Besorgen Sie sich aktionsfähige Beeinträchtigungs-Indikatoren

Für Sicherheitsteams, die Details zur Identifizierung von Systemen benötigen, bei denen Abhilfemaßnahmen ergriffen werden müssen, bietet Cyren ein Incident Management-Dashboard und detaillierte forensische Berichte, die Sicherheitsumgehungstechniken, Netzwerkaktvität, Persistenztechniken, Detektionsvermeidungstechniken, System- und Dateikonfigurationsänderungen, Speicher- und Prozessanalyse, Paketerfassungen zur detaillierten Analyse sowie Ursprungs- und Zielanalysen bei verdächtigen Orten umfassen.



Cyren Sandboxing-Incident Management-Dashboard und forensische Berichte

Funktionsweise

Cyren Sandboxing nutzt eine innovative, zum Patent angemeldete Multi-Sandbox-Array-Technologie, die von einer ausgefeilten, auf Heuristik basierenden Engine koordiniert wird, um zu gewährleisten, dass unbekannte Dateien vollständig analysiert werden, und zwar auch solche, die versuchen, einer Entdeckung zu entgehen.

1. Eine ausgetüftelte Vorverarbeitung kombiniert statische und dynamische Analysen. Daraufhin werden das erwartete Verhalten der Datei prognostiziert und eine angemessene Sandbox ausgewählt.
2. Die Datei wird bei der ausgewählten Sandbox eingereicht und auf bösartige Aktivitäten sowie das vollständige Ausdrücken aller erwarteten Verhaltensweisen überwacht.
3. Wird nicht der vollständige Satz erwarteter Verhaltensweisen festgestellt, wird die Datei rekursiv an verschiedene Sandbox-Typen gesendet, die je nach Betriebssystem, Browsertyp oder virtueller bzw. physischer Umgebung variieren können, bis das vollständige Verhalten beobachtet und ein aggregierter Bedrohungs-Score berechnet wird.
4. Wenn bösartige Dateien und URLs identifiziert wurden, nimmt Cyren davon Fingerabdrücke und blockiert sie ihn Sekundenschnelle im gesamten globalen Netzwerk, wodurch ein schützender „Netzwerkeffekt" für alle Cyren-Kunden erzielt wird.